On page 29, line 21, delete "the serial number serial number" and insert in lieu thereof --the serial number--.

Enclosed are replacement sheets for pages 16, 17, 20, 21, 29 and 30 of the specification reflecting the above amendments.

The Commissioner is hereby authorized to charge any underpayment of fees associated with this communication or credit any overpayment to Deposit Account No.04-0822.

Respectfully submitted,

DERGOSITS & NOAH LLP

Dated: January 22, 2002

By: _____
Geoffrey T. Staniford
Reg. No. 43,151

Please send all correspondence to:

Geoffrey T. Staniford
DERGOSITS & NOAH LLP
Four Embarcadero Center, Suite 1450
San Francisco, California 94111
(415) 705-6377

present invention. Figure 2B provides a more detailed illustration of the encryption process illustrated in Figure 2A. Figure 2B illustrates the encryption/decryption processes performed by a user 220 on a client computer (or "console") and a server computer 222 over a network. The server computer 222 provides a software product (also referred to as a software title) requested by the user 220. To ensure secure distribution of the software product over the network, the exchange between the user and server incorporates a multi-layered public key encryption (PKCS) to enable decryption of the software product content stored on storage media (e.g., magnetic or optical disk) by a user from a server. In general, for the process illustrated in Figure 2B, the server 222 encrypts a key that can be decrypted using a matching private key created at the client computer (console). The server 222 creates a pair of keys (User A and User B) and transmits one of the keys (User A) to the user. This key allows the user to decrypt the contents of the software product. The server encrypts this key using the key sent from the user, then re-encrypts the encrypted key with its corresponding key (User B) of the key pair, and transmits to the user the double encrypted key.

For the embodiment illustrated in Figure 5, the software title is encrypted with the title public key (Title A). To start the process, the user 220 provides user information to the server 222. The server 222 uses the user information to create a user public key (User A) and user private key (User B) pair 226. The server 222 then transmits the User A key back to the user 220. A console public key/private key pair comprising a Console A key 228 and a Console B key 229 is then created for the user 220. The user encrypts and transmits the console public key (Console A) 228 to the server 222 using the user public key (User A). The user 220 next transmits the title ID to the server 222 for the

software product to be purchased. The server 222 retrieves title private key (Title B) 232 for the specified software product. The Title B key is the private key corresponding to the title public key (Title A). The server 222 then re-encrypts and transmits the Title B key to the user 220 using the user private key (User B). The user then decrypts the encrypted software title using the title public key (Title A).

After the decryption of the software title that has been encrypted with the title public key (Title A) by the user 220, the user transmits purchase information 240 to the server 222. Using the purchase information, the server 222 creates a usage counter 242. The usage counter can be embodied in an electronic token that is debited with each use, time period, or some other unit of measure. The counter is encrypted and transmitted to the user 220 using the Console A and User B keys.

As illustrated in Figure 2A, the user public key/private key (User A/User B) pair 226 is created by the server 222, using the user information provided by the user 220. In one embodiment, one user key pair 226 is created for the user 220 for use in all subsequent transactions with server 222 in which the user information used to create the key pair is relevant. Alternatively, a new key pair 226 is created for each different transaction between user 220 and server 222.

The console public key/private key pair 228, 229 is created by the user 220. This key pair can be created on the client computer by using hardware identification means, such as the unique serial number associated with the client computer, or an ID pattern associated with the hard disk drive within the client computer. For this embodiment, the key pair can be created using authorization software that is stored and executed in the hard disk drive of the client computer. Alternatively, the key pair 228, 229 can be

with the server to purchase and receive software products. In order to access his or her account, the user calls into the server using a touch-tone phone and enters account and purchasing information using the numeric keypad on the telephone. The server system is set up with a pre-set menu to instruct the user to enter the required information to complete the purchase transaction. For example, once the user has established an account, the user is issued an ID number. In step 302, the user enters his or her user ID number using the touch-tone telephone 132.

To establish a secure connection between the client user and server, the server implements a data encryption/decryption system. Thus, in step 304, the server creates a user public key and a user private key for the user. In step 306, the server provides the user with the user public key. For the embodiment in which the user is communicating with the server over a telephone line, this information could be transmitted by a voice synthesizer which reads the user public key to the user over the phone, or by a similar arrangement. Alternatively, customer service personnel or operator could read the public key information to the user.

The packaged media containing a selection of software products is distributed to the user. This can occur generally at any time prior to the authorization process, and can be accomplished by several means, such as sending the packaged media to the customer or providing access to the media through a retailer. Using the Interactive Computer Entertainment System, the user then indicates which software title he or she would like to rent or otherwise purchase subject to limited use restrictions. The user may be presented with a menu of choices displaying the titles of programs or content available to be rented. The user enters his or her user public key into the Interactive Computer Entertainment

System, step 308. In step 310, the Interactive Computer Entertainment System encrypts the ID number of the software title to be rented into the user public key. The Interactive Computer Entertainment System also encrypts the memory card public key into the user public key. In one embodiment, the memory card public key is created based on the information stored in the memory card and is programmed into the memory card that is inserted into the Interactive Computer Entertainment System upon use. The Interactive Computer Entertainment System then displays this encrypted information on the screen of a display device coupled to the system, step 312.

The encrypted information provided to the user comprises the decryption information that the user provides to the server to verify that the user is authorized to receive and use the product. As illustrated in Figure 2A, the user can transmit the decryption information to the user either off-line or on-line depending upon whether or not the game console is coupled to the server system over a computer network. Thus, in step 316, it is determined whether the user is connected to the server through either on-line means or off-line means. If the user is not directly connected to the server (off-line), the user transmits the decryption information displayed on the screen by telephone to the server, step 318. If the game console is connected to the server through a direct communications network, the user transmits the decryption information to the server over the network line, step 320.

After the user transmits the decryption information to the server, the server verifies that the user is authorized to receive the product. In one embodiment, the server may be programmed to provide the user with a menu of choices regarding product purchase or rental options. The user is guided through a pre-determined set of menus that

allows this procedure to be accomplished a limited number of times. The same procedure could be used to allow the disc to be played on a different, rather than replacement, playback machine. By limiting the number of times a new key can be generated, it is possible to eliminate the piracy of mass producing a disk with a single serial number. Although it may still be possible for unauthorized users to create many different serial number disks, they would still need to purchase the software for each copy of the serial number. In general, this would not be cost effective as long as the limit on new keys is low (say only two replacement keys are allowed). Furthermore, additional security could be required for a replacement key. For example, if a replacement key is requested, it may be necessary for a security question to be answered or for the key to be posted to a specific physical address or e-mail or for the person to be called back, thus allowing some identification of the person requesting the replacement key.

For the above-described embodiment, the user first receives a freely distributed disk, or other program containing media that contains a sample or limited version of the software product. At the end of the free trial or demo, an instruction page is displayed which tells the user how to purchase the game instantly. Purchasing can be done on-line through the accessing a displayed URL to connect to an automated website, or off-line through calling a displayed telephone number or mailing to a displayed address or fax number. A software routine on the disk will then generate a secure key. As described above, this key can be generated from just the disk serial number or from both the disk serial number and the serial number of the playback machine, both of which can be read by the application. In one embodiment, the key is an alphanumeric string consisting of a combination of letters and numbers. They key that is generated can be used by server

computer to uniquely identify both the disk serial number and also the playback machine serial number.

When the user accesses the server computer, through either the on-line URL or off-line telephone number, he or she is asked to enter the key along with their credit card billing information. A secure database records this information and authorizes the credit card, and so on. After this step, the server generates the unlock key. The unlock key is generated as a combination of the key that user provides and a master key for that specific software application. The application is known to the server based on the disk serial number. The unlock key is stored securely in a central database, and is also an alphanumeric string of letters and numbers. Once the key is delivered to the user, and the user confirms receipt, the transaction is finished and the database records the transaction and the keys. If the user ever forgets or otherwise needs to reaccess their key, they need only to call or go on-line again, enter the disk ID key which is always presented upon booting the disk and retrieve the unlock key since the database knows that this is a legitimately purchased key.

Once the user has received the unlock key, it can be entered into the playback machine through input means, such as a keyboard or some form of virtual keyboard. The playback machine stores the unlock key in a static memory area, such as a memory card or hard disk space. Upon execution, the main application program of the purchased software product verifies that the key is authentic and correct for that specific disk and playback machine. Assuming that the key is authentic, the main application is unlocked. For added security, the main executable file can be encrypted so that it cannot easily be hacked by an unauthorized user.